Appln No. 09/886,930
Amdt date March 30, 2004
Reply to Office action of December 30, 2003

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-127. (Cancelled)

D'

1.
1~~28~~. (Currently Amended) A user authentication method for a communication network having a plurality of nodes, the method comprising:

entering on a first node first user identification information;

transmitting to an authentication agent on a second node communicating with the first node over a LAN link the first user identification information;

relaying from the authentication agent to an authentication server the first user identification information;

comparing on the authentication server the first user identification information with user identification information in a database of user identification information; and

transmitting from the authentication server to the authentication agent, if the first user identification information matches user identification information in the database of user identification information, notification information notifying the authentication agent that a user on the first node has been authenticated whereupon the

D

authentication agent authorizes transmission on the second node of packets in data flows involving the first node, wherein the first user identification information is transmitted to the authentication agent as part of a MAC-based authentication flow between an authentication client on the first node and the authentication agent.

D1

2. ~~129~~. (Previously Presented) The method of claim 1 ~~128~~, further comprising relaying from the authentication agent to the authentication client as part of the MAC-based authentication flow the notification information.

3. ~~130~~. (Previously Presented) The method of claim 1 ~~128~~, further comprising, prior to transmitting the first user identification information to the authentication agent, transmitting from the authentication client to the authentication agent as part of the MAC-based authentication flow a request to establish an authentication session.

4. ~~131~~. (Previously Presented) The method of claim 1 ~~128~~, further comprising transmitting from the authentication client to the authentication agent as part of the MAC-based authentication flow a logoff request, whereupon the authentication agent revokes the authorization.

5. ~~132~~. (Currently Amended) The method of claim 1 ~~128~~, further comprising transmitting from the authentication server to the authentication agent, if the first user identification

D

Appln No. 09/886,930
Amdt date March 30, 2004
Reply to Office action of December 30, 2003

information does not match user identification information in the database, second notification information notifying the authentication agent that the user on the first node has failed to become authenticated, whereupon the authentication agent fails to authorize transmission on the second node of packets in data flows involving the first node and relays to the authentication client as part of the MAC-based authentication flow the second notification information.

6. ~~133~~. (Previously Presented) The method of claim ~~132~~ 5, wherein if the authentication agent determines that the user has made a predetermined number of failed authentication attempts, the authentication agent transmits to the authentication client as part of the MAC-based authentication flow information notifying the authentication client that further authentication attempts will be inhibited.

7. ~~134.~~ (Previously Presented) The method of claim ~~128~~ 1, wherein the packets transmitted pursuant to the authorization are neither encrypted nor decrypted by the second node.

8. ~~135~~. (Previously Presented) A user authentication method for a communication network having a plurality of nodes, the method comprising:

entering on a first node first user identification information;

transmitting to an authentication agent on a second node communicating with the first node over a LAN link the first user identification information;

relaying from the authentication agent to an authentication server the first user identification information;

comparing on the authentication server the first user identification information with user identification information in a database of user identification information; and

transmitting from the authentication server to the authentication agent, if the first user identification information matches user identification information in the database of user identification information, information notifying the authentication agent that a user on the first node has been authenticated whereupon the authentication agent authorizes transmission on the second node of packets in data flows involving the first node, wherein the authorization comprises authorizing an interface to the LAN link to allow packets in data flows.

9. ~~136~~. (Previously Presented) The method of claim ~~135~~ 8, wherein the interface is on the second node.

10. ~~137~~. (Previously Presented) The method of claim ~~135~~ 8, wherein the LAN link is an Ethernet link.

11. ~~138~~. (Previously Presented) The method of claim ~~135~~ 8, wherein the authentication server is a RADIUS server.

Appln No. 09/886,930
Amdt date March 30, 2004
Reply to Office action of December 30, 2003

12. ~~139~~. (Previously Presented) The method of claim 8 ~~135~~, wherein the authentication server is on a third node.

13. ~~140~~. (Previously Presented) The method of claim 8 ~~135~~, wherein prior to the authorization, the second node drops all packets received from the first node that are not part of an authentication flow.

14. ~~141~~. (Previously Presented) The method of claim 8 ~~135~~, wherein prior to the authorization, the second node drops all packets received from the first node that are not addressed to the authentication agent.

15. ~~142~~. (Currently Amended) A user authentication method for a communication network having a plurality of nodes, the method comprising:

entering on a first node first user identification information;

transmitting to an authentication agent on a second node communicating with the first node over a LAN link the first user identification information;

relaying from the authentication agent to an authentication server the first user identification information;

comparing on the authentication server the first user identification information with user identification information in a database of user identification information; and

transmitting from the authentication server to the authentication agent, if the first user identification information matches user identification information in the database of user identification information, <u>notification</u> information notifying the authentication agent that a user on the first node has been authenticated whereupon the authentication agent authorizes transmission on the second node of packets in data flows involving the first node and one or more nodes reachable by the first node via the second node and relays to the first node the notification information.

16. ~~143~~. (Previously Presented) The method of claim 15 ~~142~~, wherein prior to the authorization, the second node inhibits transmission to any nodes reachable by the first node via the second node of all packets received from the first node that are not part of an authentication flow.

17. ~~144~~. (Previously Presented) The method of claim 15 ~~142~~, wherein prior to the authorization, the second node inhibits transmission to any nodes reachable by the first node via the second node of all packets received from the first node that are not addressed to the authentication agent.

18. ~~145~~. (Previously Presented) The method of claim 15 ~~142~~, further comprising, prior to transmitting the first user identification information to the authentication agent, transmitting from the first node to the authentication agent a request to establish an authentication session.

Appln No. 09/886,930
Amdt date March 30, 2004
Reply to Office action of December 30, 2003

19. ~~146~~. (Previously Presented) The method of claim ~~142~~ 15, further comprising transmitting from the first node to the authentication agent a logoff request, whereupon the authentication agent revokes the authorization.

20. ~~147~~. (Currently Amended) The method of claim ~~142~~ 15, further comprising transmitting from the authentication server to the authentication agent, if the first user identification information does not match user identification information in the database, second notification information notifying the authentication agent that the user on the first node has failed to become authenticated, whereupon the authentication agent fails to authorize transmission on the second node of packets in data flows involving the first node and any nodes reachable by the first node via the second node and relays to the first node the second notification information.

21. ~~148~~. (Previously Presented) The method of claim ~~147~~ 20, wherein upon receipt of the second notification information, the authentication agent determines the number of failed authentication attempts made by the user.

22. ~~149~~. (Previously Presented) The user authentication method of claim ~~148~~ 21, wherein if the authentication agent determines that the user has made a predetermined number of failed authentication attempts, the authentication agent inhibits further authentication attempts.

23.
~~150.~~ (Previously Presented) The user authentication method of claim ~~148~~, 21 wherein if the authentication agent determines that the user has made a predetermined number of failed authentication attempts, the authentication agent transmits to the first node information notifying the first node that further authentication attempts will be inhibited.

D

24.
~~151.~~ (Previously Presented) A user authentication method for a communication network having a plurality of nodes, the method comprising:

entering on a first node first user identification information;

transmitting to an authentication agent on a second node communicating with the first node over a LAN link the first user identification information;

relaying from the authentication agent to an authentication server the first user identification information;

comparing on the authentication server the first user identification information with user identification information in a database of user identification information; and

transmitting from the authentication server to the authentication agent, if the first user identification information matches user identification information in the database of user identification information, information notifying the authentication agent that a user on the first node has been authenticated whereupon the authentication agent authorizes transmission on the second node of packets in data flows involving the first node, wherein the packets that are

D

transmitted pursuant to the authorization bypass the authentication agent.

25.
~~152~~. (Previously Presented) A user authentication method for a communication network having a plurality of nodes, the method comprising:

entering on a first node first user identification information;

transmitting to an authentication agent on a second node communicating with the first node over a LAN link the first user identification information;

relaying from the authentication agent to an authentication server the first user identification information;

comparing on the authentication server the first user identification information with user identification information in a database of user identification information; and

transmitting from the authentication server to the authentication agent, if the first user identification information matches user identification information in the database of user identification information, information notifying the authentication agent that a user on the first node has been authenticated and information identifying a VLAN for which the user has been authenticated whereupon the authentication agent authorizes transmission on the second node of packets in data flows that involve the first node and are within the VLAN.

Appln No. 09/886,930
Amdt date March 30, 2004
Reply to Office action of December 30, 2003

26. ~~153~~. (Currently Amended) The method of claim ~~152~~ 25, wherein the information notifying the authentication agent that the user on the first node has been authenticated and the information identifying the VLAN for which the user has been authenticated are transmitted from the authentication server to the authentication agent in [the same] a single packet.

27. ~~154~~. (Previously Presented) The method of claim ~~152~~ 25, wherein one or more of the packets that are transmitted pursuant to the authorization are appended on the second node and transmitted from the second node to a backbone network with an identifier of the VLAN.

28. ~~155~~. (Previously Presented) The method of claim ~~152~~ 25, further comprising dropping on the second node of packets in data flows involving the first node and other nodes that are not within the VLAN.

29. ~~156~~. (Previously Presented) The method of claim ~~152~~ 25, further comprising, before the authorization, dropping on the second node of packets in data flows involving the first node.

30. ~~157~~. (Previously Presented) The method of claim ~~152~~ 25, further comprising, after the authorization, forwarding on the second node of packets in data flows involving the first node and other nodes that are within the VLAN.

D

Appln No. 09/886,930
Amdt date March 30, 2004
Reply to Office action of December 30, 2003

~~158.~~ 31. (Previously Presented) The method of claim ~~152~~ 25, wherein the first user identification information is transmitted from the first node to the authentication agent as part of a MAC-based authentication flow between an authentication client on the first node and the authentication agent.

~~159.~~ 32. (Previously Presented) The method of claim ~~152~~ 25, wherein the authorization comprises authorizing an interface to the LAN link to allow packets in data flows.

~~160.~~ 33. (Previously Presented) The method of claim ~~152~~ 25, wherein the packets that are transmitted pursuant to the authorization bypass the authentication agent.